that enables users to locate hosts and services, *e.g.*, a certificate management service. An example of a directory service is Lightweight Directory Access Protocol (LDAP).

[0016] LDAP is the Internet standard for directory lookups, just as the Simple Mail Transfer Protocol (SMTP) is the Internet standard for delivering e-mail, and the Hypertext Transfer Protocol (HTTP) is the Internet standard for delivering documents. Technically, LDAP is defined as an "on the wire" bit protocol (similar to HTTP) that runs over Transmission Control Protocol/Internet Protocol (TCP/IP). LDAP creates a standard way for applications to request and manage directory information.

[0017] An LDAP-compliant directory leverages a single, master directory that owns all user, group, and access control information. The directory is hierarchical, not relational, and is optimized for reading, reliability, and scalability. This directory becomes a specialized, central repository that contains information about objects and provides user, group, and access control information to all applications on the network. For example, the directory can be used to provide a security management system with a user list, a user's public key information, or user identification for all users in a widely distributed enterprise.

Summary of Invention

[0018] In general, in one aspect, the invention comprises a network system providing integration. The network system comprises a client computer, a server, a server-side cryptographic function providing cryptographic services located on the server, a PKI-Bridge providing an interface between the server and the server-side cryptographic function, a remote access switch providing an interface between the client computer and the server, a client-side cryptographic function providing cryptographic services located on the client computer, a dial-up client

providing dialing services to access the remote access switch, and a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function.

[0019] In general, in one aspect, the invention comprises a network system providing integration. The network system comprises a client computer, a server, a server-side cryptographic function providing cryptographic services located on the server, a PKI-Bridge providing an interface between the server and the server-side cryptographic function, a remote access switch providing an interface between the client computer and the server, a client-side cryptographic function providing cryptographic services located on the client computer, a dial-up client providing dialing services to access the remote access switch, a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function, a security device holding authentication information, a card reader attached to the client computer for reading the security device, and a directory service accessed by the server-side cryptographic function.

[0020] In general, in one aspect, the invention comprises a client computer. The client computer comprises a dial-up client providing dialing services to the client computer, a client-side cryptographic function providing cryptographic services located on the client computer, a custom script dynamically linked library providing an interface between the dial-up client and the client-side cryptographic function, and a card reader attached to the client computer for reading a security device.

[0021] In general, in one aspect, the invention comprises a server. The server comprises a server-side cryptographic function providing cryptographic services located on the server, a PKI-Bridge providing an interface between the server and the server-side cryptographic function, and a directory service accessed by the server-side cryptographic function.

[0022] In general, in one aspect, the invention comprises a method of integrating via a dial-up interface. Session initiation information is sent from a dial-up client to a PKI-Bridge. Session initiation information is checked by the PKI-Bridge. A challenge string is generated by a server-side cryptographic function. The challenge string is forwarded to a custom script dynamically linked library. The challenge string is forwarded to a client-side cryptographic function from the custom script dynamically linked library. A private key is retrieved from a security device. A response string is generated. The response string is signed with the private key of a dial-in user. A signed response string is forwarded to the custom script dynamically linked library. The signed response string is divided into packets. Packets are forwarded to the PKI-Bridge. The signed response string is reconstructed from packets. A reconstructed signed response string is forwarded to the server-side cryptographic function. A public key of the dial-in user is obtained. The reconstructed signed response string is verified using the server-side cryptographic function.

[0023] In general, in one aspect, the invention comprises a method of integrating via a dial-up interface. Session initiation information is sent from a dial-up client to a PKI-Bridge. Session initiation information is checked by the PKI-Bridge. A challenge string is generated by a server-side cryptographic function. The challenge string is forwarded to a custom script dynamically linked library. The challenge string is forwarded to a client-side cryptographic function from the custom script dynamically linked library. A private key is retrieved from a security device. A response string is generated. The response string is signed with the private key of a dial-in user. A signed response string is forwarded to the custom script dynamically linked library. The signed response string is divided into packets. Packets are forwarded to the PKI-Bridge. The signed response string is reconstructed from packets. A reconstructed signed response string is forwarded to the server-side cryptographic function. A public key of the dial-in